Prof. Friedrich Eisenbrand
Nicolai Hähnle

Discussions from: May 24, 2011

Computer Algebra

Spring 2011

Assignment Sheet 7

Due to the coming end of the ~~world~~semester, these exercises are for your own enjoyment (and exam preparation) only. There will be no bonus points.

Exercise 1

Let $\Lambda \subset \mathbb{R}^n$ be a full-dimensional lattice and define the *dual lattice*

$$\Lambda^\star = \{y \in \mathbb{R}^n \mid y^T x \in \mathbb{Z} \text{ for all } x \in \Lambda\}$$

1. Prove that $\Lambda^\star$ is a lattice and that $(\Lambda^\star)^\star = \Lambda$.
2. Let B be a basis of Λ. Prove that B^{-T} is a basis of $\Lambda^\star$.
3. Let $y \in \Lambda^\star$ be arbitrary and consider the affine hyperplanes $H_k = \{x \in \mathbb{R}^n \mid y^T x = k\}$ for all $k \in \mathbb{Z}$. Prove that $\Lambda \subset \bigcup_{k\in\mathbb{Z}} H_k$.
4. Let U be an $(n-1)$-dimensional subspace of $\mathbb{R}^n$ so that $\Lambda' := \Lambda \cap U$ is an $(n-1)$-dimensional lattice with basis $b_1, \ldots, b_{n-1}$.
   a) Prove that there exists $y \in \Lambda^\star$ such that $U = \{x \in \mathbb{R}^n \mid y^T x = 0\}$ and $\frac{1}{k} \cdot y \notin \Lambda^\star$ for all integers $k \geq 2$.
   b) Consider the affine lattice hyperplane $H = \{x \in \mathbb{R}^n \mid y^T x = 1\}$. Prove that $H \cap \Lambda$ is non-empty.
   c) Let $w \in H \cap \Lambda$ be arbitrary. Prove that $b_1, \ldots, b_{n-1}, w$ is a basis of Λ.

Exercise 2

For a full-dimensional lattice $\Lambda \subset \mathbb{R}^n$, we say that $v_1, \ldots, v_n$ is a sequence of shortest independent vectors if v_j is a shortest vector in $\Lambda \setminus \langle v_1, \ldots, v_{j-1}\rangle$. In particular, v_1 is a shortest non-zero lattice vector.

1. Prove that a sequence of shortest independent vectors always exists, and that $v_1, \ldots, v_n$ span all of $\mathbb{R}^n$, i.e., they are linearly independent.
2. Prove that the sequence $\lambda_1 := \|v_1\|, \ldots, \lambda_n := \|v_n\|$ is independent of the choice of shortest independent vectors. In other words, the λ_j are a property of the lattice.
3. Let $n = 2$. Prove that a sequence of shortest independent vectors is a basis of the lattice.

4. Prove that, for $n \geq 4$, a sequence of shortest independent vectors is not necessarily a lattice basis.

   Hint: Consider the *parity lattice* $\Lambda = \{x \in \mathbb{Z}^n \mid x_1 \equiv \cdots \equiv x_n \pmod 2\}$. Prove that it is a lattice. Then find a sequence of shortest independent vectors that is not a basis. It probably helps to first find a basis of the lattice.

Exercise 3

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. Our goal is to find good approximations of those numbers using a common denominator $q \in \mathbb{N}$. Consider the lattice Λ generated by the basis

$$\begin{pmatrix} N & 0 & \ldots & 0 & -\alpha_1 \cdot N \\ 0 & N & & 0 & -\alpha_2 \cdot N \\ & & \ddots & \vdots & \vdots \\ \vdots & & & N & -\alpha_n \cdot N \\ 0 & 0 & \ldots & 0 & N^{-n} \end{pmatrix}$$

where $N \in \mathbb{N}_{\geq 2}$.

1. Prove that there is a non-zero vector $(p_1, \ldots, p_n, q) \in \Lambda \cap [-1,1]^{n+1}$ with $q \geq 1$.
2. Prove that $q \leq N^n$ and $|\frac{p_j}{q} - \alpha_j| \leq \frac{1}{qN}$ for all $j = 1 \ldots n$.
3. Determine the best possible guarantee you can get for an approximate shortest vector returned by the LLL algorithm.

Exercise 4

Let $\alpha_1, \ldots, \alpha_n \in (0,1]$. Use lattice techniques to prove a statement of the form: there exist $x_1, \ldots, x_n \in \mathbb{Z}$, $|x_1|, \ldots, |x_n| \leq N$, not all zero, such that $|\alpha_1 x_1 + \ldots + \alpha_n x_n| \leq f(n, N)$, with $f(n, N)$ being as small as possible.

Let α be an (approximation of an) algebraic number of degree n over $\mathbb{Q}$. Setting $\alpha_j := \alpha^{j-1}$, consider how the above can be adapted to find the minimal polynomial of α. (The minimal polynomial $p \in \mathbb{Q}[x]$ is the unique monic polynomial of smallest degree that has α as a root.)